IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

UNITED STATES OF AMERICA	**)**	
	)	
v.	**)**	**Case No. 3:19cr19**
	)	
TROY GEORGE SKINNER,	**)**	
Defendant	**)**	

SUPPLEMENTAL BRIEF REGARDING MOTION TO SUPPRESS EVIDENCE

Troy Skinner, through counsel, supplements his Motion to Suppress Evidence as follows:

I. ***The facts in this case demonstrate that these warrants were general warrants.***

In his Motion to Suppress, Mr. Skinner challenged as overbroad and lacking in particularity three warrants that sought access to his electronic information. The first warrant, which was admitted as Government Exhibit 1 at the suppression hearing, authorizes the search of Mr. Skinner's cell phones—specifically at issue here the search of his Huawei cell phone. The second warrant, which was admitted as Government Exhibit 2 at the suppression hearing, authorizes the search of Mr. Skinner's "vlogchamber" Google account. The third warrant, which was admitted as Government Exhibit 3 at the suppression hearing, authorizes the search of Mr. Skinner's "lottic" Google account. Each of these warrants authorizes the search for and seizure of evidence far beyond the scope of probable cause that the affiants set forth in their applications to search and seize Mr. Skinner's property.

a. Government Exhibit 1

In Government Exhibit 1, Attachment B lists out the "property to be seized," which as paragraph 2 of Attachment B indicates includes the entire phone. Many of the paragraphs—*see* Attachment B, paragraphs 1(a), 1(b), 1(c), 1(e), 1(f), and 1(g)—relate to a purported child

pornography collector profile. As discussed further below, the evidence presented to the magistrate about Mr. Skinner did not match that profile. Several other paragraphs—*see* Attachment B, paragraphs 1(h) and 3—have no relation to the scope of probable cause and relevant timeframe of this case. The warrant itself authorizes the search and seizure of the entire phone without limit.

As it relates to the child pornography production charges, the affidavit in Government Exhibit 1 describes an online relationship between Mr. Skinner and the young woman in this case. The two exchanged pictures and videos of each other online. There is no indication at all in the affidavit that Mr. Skinner was interested in the young woman for any other reason than what was in his mind a sincere friendship that turned into a sincere romantic relationship. While there is probable cause in the affidavit to believe that the young woman was a minor and therefore any sexually explicit pictures of her constituted child pornography under the laws of the United States, there is no indication at all in the affidavit that Mr. Skinner was interested in any other minors or even had any contact with any other minors.

The affidavit contains generic language that the agent took verbatim from other warrants about "characteristics of collectors of child pornography." *See* Gov't Ex. 1 at ¶¶17-24. This profile section relates that "collectors" of child pornography have common characteristics. For example, the profile alleges that child pornography collectors "receive sexual stimulation and satisfaction from contact with children;" collect child pornography in a variety of media including "photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media;" "almost always" maintain their child pornography collections in a "private and secure location;" correspond with other child pornography collectors; keep their child pornography near them at all times; and subscribe to particular websites designed to distribute child

pornography. *Id.* The affidavit does not indicate in any way that Mr. Skinner possessed or displayed any of these characteristics.

Rather, what the affidavit describes is a sincere, online friendship between Mr. Skinner and one young woman that developed into a sincere, online romantic relationship that became sexually explicit. The affidavit indicates that the virtual platform for the online relationship was in the gaming application Discord. *Id.* at ¶¶14(i), 33-34, 36-38. The affidavit further states that Mr. Skinner told the young woman that he used Discord on his cell phone and on his home computer. *Id.* at ¶34. Thus, the scope of probable cause that the affidavit gives rise to is for law enforcement to search Mr. Skinner's cell phone and seize information from his Discord account relating to his sexually explicit relationship with the young woman as well as sexually explicit picture and video files of the young woman.

Nowhere, however, does Attachment B provide any limits to the search of Mr. Skinner's phone for the seizure of such evidence. Rather, Attachment B authorizes the seizure of "[a]ny and all visual depictions of minors" and "[a]ny and all communications with minors" anywhere on the phone. *See* Attachment B, paragraphs 1(a) and 1(b). Attachment B then authorizes the seizure of the entire phone. *See* Attachment B, paragraph 2. As explained further below, the warrant authorizes an unjustified fishing expedition that unreasonably invaded Mr. Skinner's privacy.

As Agent Weber testified, the FBI downloaded and kept the entire contents of the phone. *See* 2/13/20 Tr. at 61. The contents of the phone included call records going back to 2015, instant message chats going back to January 2014, emails going back to 2012, and internet browsing history from 2014. *Id.* at 61-62. The extraction report was 1,316 pages long and contained the video described in Count Seven of the superseding indictment. The FBI took no steps to partition

off any part of the phone or search through the phone and download files responsive to the scope of probable cause. Rather, the FBI downloaded and kept the entire contents of the phone.

b. Government Exhibit 2

In Government Exhibit 2, Attachment B lists out the "particular things to be seized," which as paragraph II(h) of Attachment B indicates includes the entire account. Many of the paragraphs in Attachment B—*see* Gov't Ex. 2, Attachment B, paragraphs II(c), II(d), II(i), and II(j)—are identical or similar to the paragraphs in Attachment B of Government Exhibit 1 seeking evidence related to a purported child pornography collector profile. *Compare* Gov't Ex. 1, Attachment B, paragraphs 1(a), 1(b), 1(c), 1(e), 1(f), and 1(g). Unlike Government Exhibit 1, the affidavit in Government Exhibit 2 does not include any generic language regarding "characteristics of collectors or child pornography." Even if it had, as discussed above, the evidence presented to the magistrate about Mr. Skinner did not match that profile. Several other paragraphs—*see* Gov't Ex. 2, Attachment B, paragraphs II(a), II(b), II(h), and II(k)—have no relation to the scope of probable cause in this case. The warrant itself authorizes the search and seizure of the entire account without limit.

Just as in Government Exhibit 1, as it relates to the child pornography production charges, the affidavit in Government Exhibit 2 describes an online relationship between Mr. Skinner and the young woman in this case. The two exchanged pictures and videos of each other online. There is no indication at all in the affidavit that Mr. Skinner was interested in the young woman for any other reason than what was in his mind a sincere friendship that turned into a sincere romantic relationship. While there is probable cause in the affidavit to believe that the young woman was a minor and therefore any sexually explicit pictures of her constituted child pornography under the

laws of the United States, there is no indication at all in the affidavit that Mr. Skinner was interested in any other minors or even had any contact with any other minors.

As in Government Exhibit 1, what the affidavit in Government Exhibit 2 describes is a sincere, online friendship between Mr. Skinner and one young woman that developed into a sincere, online romantic relationship that became sexually explicit. The affidavit indicates that there was one particular video file on Mr. Skinner's cell phone searched pursuant to Government Exhibit 1 that was downloaded from Mr. Skinner's "vlogchamber" Google account on June 19, 2018. *See* Gov't Ex. 2, Aff. ¶40. Thus, the scope of probable cause that the affidavit gives rise to is for law enforcement to search Mr. Skinner's "vlogchamber" Google account and seize information relating to sexually explicit image files of the young woman.

Nowhere, however, does Attachment B provide any limits to the search of Mr. Skinner's "vlogchamber" Google account for the seizure of such evidence. Rather, Attachment B authorizes the seizure of "[a]ll records or other information stored by an individual using the account." *See* Gov't Ex. 2, Attachment B, paragraph II(h). The warrant authorizes an unjustified fishing expedition that unreasonably invaded Mr. Skinner's privacy.

While the warrant purported to limit the seizure of evidence from the "vlogchamber" Google account "occurring after December 25, 2017, until the date of the warrant," *see* Gov't Ex. 2, Attachment B, paragraph II, as Agent Weber testified, the FBI downloaded and kept the entire contents of the "vlogchamber" Google account. *See* 2/13/20 Tr. at 69-70. The contents of the two Google accounts (both the "vlogchamber" and "lottic" accounts) seized contained 58,776 files, including 7,057 documents; 37,450 emails; 3,825 graphics; and 4,750 multimedia files. *Id.* at 70. The FBI made no efforts to limit its seizure to files responsive to the warrant created after December 25, 2017. The FBI took no steps to partition off any part of the account or search

through the account and return or delete files that were not responsive to the scope of probable cause. Rather, the FBI downloaded and kept the entire contents of the "vlogchamber" Google account. 2/13/20 Tr. at 70-71.

c. Government Exhibit 3

The contents of the affidavit and attachments to the warrant in Government Exhibit 3 are identical to the affidavit and attachments in Government Exhibit 2. The affidavit in Government Exhibit 3 indicated that there was a draft email in the "lottic" Google account on Mr. Skinner's cell phone searched pursuant to Government Exhibit 1 dated June 7, 2018, that had the young woman's home address. *See* Gov't Ex. 3, Aff. ¶41. The affidavit also indicates that there were email communications in the "lottic" Google account on Mr. Skinner's cell phone searched pursuant to Government Exhibit 1 dated June 16, 2018, that contained Mr. Skinner's travel itinerary to the United States. *See* Gov't Ex. 3, Aff. ¶42. Thus, the scope of probable cause that the affidavit gives rise to is for law enforcement to search Mr. Skinner's "lottic" Google account and seize information relating to his travel to the United States in June 2018.

Nowhere, however, does Attachment B provide any limits to the search of Mr. Skinner's "lottic" Google account for the seizure of such evidence. Rather, Attachment B authorizes the seizure of "[a]ll records or other information stored by an individual using the account." *See* Gov't Ex. 3, Attachment B, paragraph II(h). As explained further below, the warrant authorizes an unjustified fishing expedition that unreasonably invaded Mr. Skinner's privacy.

Also, just like the affidavit in Government Exhibit 2, the affidavit in Government Exhibit 3 does not include any generic language regarding "characteristics of collectors or child pornography." Even if it had, as discussed above, the evidence presented to the magistrate about Mr. Skinner did not match that profile. Just like the information seized pursuant to Government

Exhibit 2, the FBI took no steps to partition off any part of the "lottic" account or search through the account and return or delete files that were not responsive to the scope of probable cause. Rather, the FBI downloaded and kept the entire contents of the "lottic" Google account. 2/13/20 Tr. at 70-71.

II. The warrants in this case were unconstitutional general warrants.

The warrants described above are general warrants. They had no limit to the information that the government could search for and seize from the intensely private digital diaries contained within Mr. Skinner's cell phones and Google accounts. As the Supreme Court has recognized, the "sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions." *Riley v. California*, 134 S. Ct. 2473, 2489 (2015). "[T]here is an element of pervasiveness that characterizes cell phones but not physical records. Prior to the digital age, people did not typically carry a cache of sensitive personal information with them as they went about their day. Now it is the person who is not carrying a cell phone, with all that it contains, who is the exception." *Id.* at 2490. "A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is." *Id.* at 2491. The extent of the privacy interests at stake here cannot be understated.

Courts around the country have recognized that warrants such as those in Government Exhibits 1, 2, and 3 are general warrants. For example, in *In re Search of Google Email Accounts Identified in Attachment A*, 92 F. Supp. 3d 944, 946 (D. Alaska 2015), a federal magistrate judge denied an application for a search warrant that sought to allow federal agents to peruse "other email content regardless how remote or how unrelated that content may be to the current

investigation." After observing that "the rise of personal computing and networking has heightened the risk of overbroad warrants," the court went on to observe that:

> In constitutional terms, the balancing of the interests of personal privacy with the government's need to investigate criminal conduct in the information age boils down to this important question: does permitting unrestricted access to over-seized data improperly bring constitutionally protected data within the plain view exception of the warrant requirement and transform electronic data search warrants into general warrants? The answer depends on whether, given the facts of a particular case, over-seizure/over-searching can be avoided.

Id. at 951 (relying on *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162 (9th Cir. 2010))[1]. Turning to the facts at issue in *In re Search of Google Email Accounts*, the court found that there was probable cause to believe that the email responses that the government sought contained evidence of a crime—soliciting unlawful sexual contact with minors. *Id.* at 952. But:

> the scope of the government's authority to search and seize under the warrant is not tailored to its probable cause showing. A warrant is overbroad if it expands the scope of the government's search beyond the places implicated by the probable-cause showing. Here, the warrant sought by the government is overbroad because it would authorize the government to seize and search the entirety of the six Gmail accounts, even though the government has only established probable cause to look at a small number of emails within a narrow date range.

Id. The court denied the application for the search warrant and observed that the government had two options: seek an order to compel Google to comply with the terms of a narrower warrant or agree to seal without reviewing all material that was outside of the time period established by probable cause. *Id.* at 954.

[1] In *Comprehensive Drug Testing*, the Ninth Circuit sitting en banc observed that if the decision of how much evidence to seize is left in the hands of investigating agents, "this will create a powerful incentive for them to seize more rather than less: Why stop at the list of all baseball players when you can seize the entire Tracey Directory? Why just that directory and not the entire hard drive? Why just this computer and not the one in the next room and the next room after that? Can't find the computer? Seize the Zip disks under the bed in the room where the computer once might have been. Let's take everything back to the lab, have a good look around and see what we might stumble upon." *Id.* at 1171 (internal citation omitted). This case was overruled in part on other grounds as recognized by *Demaree v. Pederson*, 887 F.3d 870, 876 (9th Cir. 2018)), but remains good law for its relevance here.

Similarly, in *United States v. Winn*, 79 F. Supp. 3d 904 (S. D. Ill. 2015), the court suppressed evidence from an overbroad cell phone search warrant. The court observed that "[t]he major, overriding problem with the description of the object of the search—'any or all files'—is that the police did not have probable cause to believe that everything on the phone was evidence of the crime of public indecency." *Id.* at 919. The vast majority of the information that the warrant sought was not supported by probable cause in the affidavit. The court found that:

> The bottom line is that is [the detective] wanted to seize every type of data from the cell phone, then it was incumbent upon him to explain in the complaint how and why each type of data was connected to [the defendant's] criminal activity, and he did not do so. Consequently, the warrant was overbroad, because it allowed the police to search for and seize broad swaths of data without probable cause to believe it constituted direct evidence of public indecency.

Id. at 920. The court found that no reasonably well-trained officer would have thought that such a wholesale search was constitutional, declined to apply the good faith exception, and suppressed the evidence seized pursuant to the general warrant. *Id.* at 924, 926-27; *see also In Matter of Search of Information Associated with Facebook Account*, 21 F. Supp. 3d 1, 5-6, 11-12 (D.D.C. 2013) (narrowing scope of overbroad warrant that government sought, listing minimization procedures other courts have suggested or required, and warning that "[i]f the government cannot adopt stricter search parameters in future applications, it may find this Court unwilling to issue any search and seizure warrants for electronic data that ignore the constitutional obligations to avoid 'general' electronic warrants that are as offensive to the Fourth Amendment as the searches that led to its enactment"); *United States v. Cioffi*, 668 F. Supp. 2d 385 (E.D.N.Y. 2009) (suppressing evidence obtained from overbroad warrant for Google account information).

At the suppression hearing in the instant case, the Court asked defense counsel about the application of *United States v. Williams*, 592 F.3d 511 (4th Cir. 2010), to the instant case. In *Williams*, the Fourth Circuit evaluated a challenge to evidence of child pornography seen in "plain

view" during the execution of a search warrant that Mr. Williams argued did not allow law enforcement officials to search for evidence of child pornography. *Id.* at 517. After finding that there was probable cause to search Mr. Williams' computers for evidence of alleged threats of bodily harm and computer harassment, the Fourth Circuit observed that when a search requires reviewing a large collection of items for responsive materials, there may be "at least cursorily" an innocuous search of innocent materials to determine what may be seized. *Id.* at 519-20 (quoting *Andresen v. Maryland*, 427 U.S. 463, 482 n.11 (1976)). "If, in those circumstances, documents not covered by the warrant are improperly seized, the government should promptly return the documents or the trial judge should suppress them." *Williams*, 592 F.3d at 520.

In *Williams*, because the search at issue was of Mr. Williams' computer, "the warrant impliedly authorized officers to open each file on the computer and view its contents, at least cursorily, to determine whether the file fell within the scope of the warrant's authorization . . . ." 592 F.3d at 521. This cursory search of all files was authorized because the search warrant sought evidence of files on a computer, which could easily be manipulated and renamed to hide their criminality. *Id.* at 522.

The facts and issues in *Williams* do not square with those in this case. First, as noted above, law enforcement officials in this case did not "cursorily" review the files supported by probable cause and then return or delete the nonresponsive data. They searched and permanently seized the entire contents of Mr. Skinner's phone and Google accounts, much of went back years before the conduct at issue in this case even happened. Second, the facts of the case in *Williams*—where the allegations were that Mr. Williams self-identified as a pedophile who used several email accounts to detail his intended sexual abuse of many children at a local church—are far broader than those at issue in this case. Here, the only information presented to the magistrate was that Mr. Skinner

traded a handful of images and videos with a young woman with whom he had had an online relationship. The scope of probable cause in *Williams* gave rise to a broader search of files. Third, unlike computer files where the user has a chance to name or rename particular files to hide them, there is no such opportunity for cell phone data or data found on a Google drive.

Had the government submitted a warrant application that properly limited the information sought to that for which probable cause existed and then come across files in those categories (the relevant Discord communications and images/videos in the phone warrant and the relevant video file and emails in the Google warrants) that were clearly criminal in nature, then the plain view exception would apply to those files. But, that is not what happened in this case. In this case, the FBI seized the entire contents of Mr. Skinner's phone and Google accounts and did absolutely nothing to try to limit its unreasonable invasion of Mr. Skinner's privacy. Like the warrants at issue in *In re Search of Google Email Accounts*, *Winn*, and *In Matter of Search of Information Associated with Facebook Account*, the warrants in this case were general warrants, which are void *ab initio* and for which the Fourth Amendment was passed to abolish. The overbreadth is so pervasive as to prevent severance. *See United States v. Sells*, 463 F.3d 1148, 1151 (10th Cir. 2006). And no executing officer could have relied in good faith on warrants that purported to authorize wholesale seizures of information so far beyond the scope of probable cause.

To the extent that the government continues to rely on cases it cited in its response arguing that the affidavits attached to the warrants provided a meaningful limitation to the overbreadth in the attachments to the warrant, the Court should reject that argument. *See* Gov't Response at 8-9. As discussed above, the FBI made no effort at all to limit its seizure of evidence from Mr. Skinner's cell phones and Google accounts. Rather, the FBI seized and maintains to this day tens of thousands of files of Mr. Skinner's private data, much of which was created long before the

conduct at issue in this case. There were no limits, which proves the constitutional unreasonableness of the searches.

III. The extended seizure of Mr. Skinner's cell phone before obtaining search warrant was unreasonable.

At the suppression hearing, Agent Weber testified that the bulk of the cell phone search warrant affidavit was something she was able to cut and paste from previous warrants or copy from statutes. *See* 2/13/20 Tr. at 47-50. The only section drafted out of whole cloth in the cell phone affidavit was paragraphs 31 through 43. *Id*. at 50. She testified that it took her a couple of hours over a couple of days to draft that section. *Id.* at 50-51. She also testified that the reason that the FBI got involved in the case initially on June 23, 2018, was for the express purpose of the FBI helping the local law enforcement officials obtain a warrant to search Mr. Skinner's cell phones. *Id.* at 51-52. There were about ninety to one hundred FBI agents working in the Richmond Division at that time, all of whom had been trained in writing search warrants. *Id.* at 46, 54. Agent Weber offered no persuasive reason to justify the twenty-nine day between seizing the evidence and obtaining a search warrant for it.

As the Eleventh Circuit observed in *United States v. Mitchell*, 565 F.3d 1347, 1352 (11th Cir. 2009), "[t]he purpose of securing a search warrant soon after a suspect is dispossessed of a closed container reasonably believed to contain contraband is to ensure its prompt return should the search reveal no such incriminating evidence, for in that event the government would be obligated to return the container (unless it had some other evidentiary value). In the ordinary case, the sooner the warrant issues, the sooner the property owner's possessory rights can be restored if the search reveals nothing incriminating." As in *United States v. Pratt*, 915 F.3d 266, 272 (4th Cir. 2019), the FBI's resources were not overwhelmed here. Mr. Skinner did nothing to diminish his privacy interest in his phone, and as such, his expectation of privacy in his phone remained

robust. Just as in *Pratt*, a twenty-nine day delay between the seizure and obtaining the search warrant "violates the Fourth Amendment where the government neither proceeds diligently nor presents an overriding reason for the delay." *Pratt*, 915 F.3d at 273. The Court should suppress the contents of Mr. Skinner's cell phone that the government illegally seized.

CONCLUSION

Thus, as set forth above and in the original motion and reply, the Court should suppress images and videos the government obtained from Mr. Skinner's Google accounts and his cell phone in violation of the Fourth Amendment.

Respectfully submitted,
TROY GEORGE SKINNER

By: _____/s/_____

Laura Koenig
Va. Bar No. 86840
Counsel for Defendant
Office of the Federal Public Defender
701 E Broad Street, Suite 3600
Richmond, VA 23219-1884
Ph. (804) 565-0881
Fax (804) 648-5033
laura_koenig@fd.org

Robert Wagner
Va. Bar No. 27493
Office of the Federal Public Defender
701 East Broad Street, Suite 3600
Richmond, VA 23219
Ph. (804) 565-0808
Fax (804) 648-5033
robert_wagner@fd.org

CERTIFICATE OF SERVICE

I hereby certify that on March 4, 2020, I filed the foregoing with the Clerk of Court using the CM/ECF system, which will send a notification of such filing (NEF) to all counsel of record.

_____/s/_____
Laura Koenig
Va. Bar No. 86840
Counsel for Defendant
Office of the Federal Public Defender
701 E Broad Street, Suite 3600
Richmond, VA 23219-1884
Ph. (804) 565-0881
Fax (804) 648-5033
laura_koenig@fd.org